Mechanism of Homomorphic Encryptions (Algorithmic and Computational Theory in Algebra and Languages)

AUTHOR(S):

Yamamura, Akihiro

CITATION:

Yamamura, Akihiro. Mechanism of Homomorphic Encryptions (Algorithmic and Computational Theory in Algebra and Languages). 数理解析研究所講究録 2008, 1604: 31-36

ISSUE DATE:

2008-06

URL:

http://hdl.handle.net/2433/139935

数理解析研究所講究録
第1604巻 2008年 31-36

Mechanism of Homomorphic Encryptions *

Akihiro Yamamura
Department of Computer Science and Engineering
Akita University
1-1, Tegata gakuen-machi, Akita-shi, Akita 010-8502, Japan
email: yamamura@ie.akita-u.ac.jp

Abstract

We study mechanism, design principles, generalization and applications of homomorphic encryptions. Our method is based on the terminology of basic group theory and nicely covers the mechanism and the security of many homomorphic encryptions.

1 Introduction

A mapping between algebraic systems is called a *homomorphism* if it preserves the algebraic structures. In cryptography, a trapdoor one-way homomorphism between cyclic groups have been studied and applied to many cryptographic protocols. Such encryptions include ElGamal, Goldwasser-Micali, Paillier, Okamoto-Uchiyama cryptosystems and so on [1, 2, 3, 4, 5]. Homomorphic encryptions share many similarities, however, no uniform mechanism has been presented so far. In this paper, we study homomorphic encryptions from the standpoint of group theory, in particular, we use split exact sequences and the subgroup membership problem to explain the mechanism, constructions and the indistinguishability of homomorphic encryptions.

Our contribution in this paper is to explain the mechanism of homomorphic encryptions using uniform design via exact sequences and the subgroup membership problem. This is presented in Yamamura[7] and security discussions are given in [6, 8, 9]. This approach simplifies the mechanism of numerous homomorphic encryptions and enable us to explain functionality of homomorphic encryptions in a mathematically sound way.

2 Mechanism of Homomorphic Encryptions

We describe the mechanism of homomorphic encryption functions. First, we recall that a sequence of homomorphisms $1 \longrightarrow H \xrightarrow{\delta} G \xrightarrow{d} P \longrightarrow 1$ is called *exact* if the kernel Ker$d$ coincides with the image Imδ. Following the mathematical convention, "1" stands for the trivial subgroup $\{1\}$. If the group operation is additive, we may denote it by 0. Note that $\delta : H \to G$ is an embedding and $G \to P$ is surjective. Furthermore, if there exists a homomorphism $\epsilon : P \to G$ such that $d \circ \epsilon$ is the

*This paper is an extended abstract and the detailed version will be published elsewhere.

identity mapping of P, then we say that the exact sequence *splits*. In such a case, G is isomorphic to a semidirect product of H by P.

Let k be the security parameter. For the input 1^k, a probabilistic polynomial time algorithm $\mathcal{IG}$, called an *instance generator*, outputs the description of a finite group P, the description of a finite group G, the description of a subgroup H of G, the couple of public and private keys, and the description of a probabilistic algorithm $\mathcal{SAM}$, called a sampling algorithm, that chooses randomly and uniformly an element of H. Elements in G and P are represented by binary strings and operations in the groups, multiplication and taking inverses, are efficiently computable. The subgroup H is called the *subgroup of randomizers*. The group P is called the *group of plaintexts*. The *encoder* ϵ is an isomorphism of P into G, and there is an algorithm to compute ϵ efficiently with the public key. The *decryption function* d is a homomorphism of G onto P such that $d \circ \epsilon = id_P$ and its kernel $\mathrm{Ker}\, d$ coincides with H. Furthermore, d is efficiently computable with the private key. In such a case, by the basic algebra, we have a split exact sequence $1 \longrightarrow H \xrightarrow{\delta} G \overset{\xi}{\underset{\epsilon}{\rightleftarrows}} P \longrightarrow 1$. Then $G = H\epsilon(P)$ and $H \cap \epsilon(P) = 1$. This implies that G is a semidirect product of H and $\epsilon(P)$. Furthermore, $G = \epsilon(P) \times H \cong P \times H$ and $P \cong G/H$ and $\epsilon(P)$ is the set of representatives of H in G, that is, $G = \epsilon(m_0)H \cup \epsilon(m_1)H \cup \cdots \cup \epsilon(m_n)H$, where $P = \{m_0, m_1, \ldots, m_n\}$ (if P is finite).

Encryption: The encryption function e is computed by

$$e(m) = \epsilon(m)r \ , \tag{2.1}$$

where r is an output of $\mathcal{SAM}$ and m is a plaintext in P. We note that each coset $\epsilon(m)H$ is the set of ciphertexts of the plaintext m. This means that e can be considered a probabilistic algorithm choosing an element randomly and uniformly from $\epsilon(m)H$ for each plaintext $m \in P$.

Decryption: The decryption is done just by computing d provided the private key (secret information) is given. Since $\mathrm{Ker}\, d$ coincides with H and $d \circ \epsilon = id_P$, we have $d(e(m)) = d(\epsilon(m)r) = d(\epsilon(m))d(r) = id_P(m) = m$ for every ciphertext $m \in P$. Hence, d decrypts the ciphertext $e(m)$. Note that we need the private key to compute d.

Assumption:

Let G be a group, and let H be its subgroup. The membership problem is to decide whether or not a given element g in G belongs to H. Furthermore, we consider a family of finite groups indexed by a parameter and the asymptotic behavior according to computation. In such a case, the subgroup membership is described as a computation problem to decide the membership when given an element, a subgroup and a group indexed by a parameter. A computation problem is hard if no efficient algorithms. The efficiency is characterized by the asymptotic behavior of an algorithm.

We suppose that every element in G has a binary representation of size k, where k is the security parameter. The membership can be decided within polynomial time in k if a certain information, called a *trapdoor*, is provided. The membership of an element g in G in H can be decided provided the trapdoor, however, the membership cannot be decided with a probability substantially larger than one half without the trapdoor. We now formalize the subgroup membership problem.

Let k be the security parameter. For the input 1^k, a probabilistic polynomial time algorithm $\mathcal{IG}$ outputs the description of a group G, the description of a subgroup H of G and the trapdoor that provides a polynomial time algorithm for the subgroup membership problem of H in G. The

algorithm $\mathcal{IG}$ is called the *instance generator*. Every element of G is represented as a binary sequence of length k. Computation of the multiplication in G is performed in polynomial time in k.

The predicate for the membership of a subgroup is denoted by Mem, that is, Mem is defined as follows.

$$\mathrm{Mem}(G, H, x) = \begin{cases} 1 & \text{if } x \text{ lies in } H \\ 0 & \text{if } x \text{ lies in } S \end{cases},$$

where $\mathcal{IG}$ outputs the pair (G, H) for 1^k, x is in G, and $S = G \setminus H$. The *subgroup membership problem* is to compute Mem in polynomial time in k when we inputs 1^k and obtain a pair of groups (G, H) and an element g in G, which is uniformly and randomly chosen from H or G according to the coin toss $b \stackrel{R}{\leftarrow} \{0, 1\}$. If there does not exist a probabilistic polynomial time algorithm that computes Mem with a probability substantially larger than $\frac{1}{2}$, then we say that the membership problem is *intractable.*

It is shown in [9] that the quadratic residue problem and the decision Diffie-Hellman problem can be characterized as a subgroup membership problem. We briefly review these two problems.

Quadratic Residue Problem: Let p, q be primes. Set $N = pq$. The primes p and q are trapdoor information for the quadratic residue problem, on the other hand, the integer N is a public information. Let G be the subgroup of $(\mathbb{Z}/(N))^*$ consisting of the elements whose Jacobi symbol is 1, and let H be the subgroup of G consisting of quadratic residues of G, that is, $H = \{x \in G \mid x = y^2 \bmod N \text{ for } y \in (\mathbb{Z}/(N))^*\}$. The *quadratic residue problem* (QR for short) of H in G is to decide whether or not, a given element $g \in G$, g belongs to H. We can effectively determine the membership of g in H provided that the information p and q are available. No polynomial time algorithm is known for the membership of a randomly chosen element of G in H without the information p and q. Hence, if we define an instance generator for the QR problem as a probabilistic algorithm that outputs two primes p and q of size k and a quadratic non-residue h whose Jacobi symbol is 1 for the input 1^k, then the QR problem is considered as a subgroup membership problem.

Decision Diffie-Hellman Problem: Let C be a cyclic group of prime order p. Let g be a generator of C. The *decision Diffie-Hellman problem* (DDH for short) is to decide whether or not $h_2 = g_2^a$ for the given quadruple (g_1, h_1, g_2, h_2) of elements in C with $h_1 = g_1^a$ for some $1 \leq a \leq p-1$. If so, we say that (g_1, h_1, g_2, h_2) is a Diffie-Hellman quadruple. The integer a is the trapdoor of the DDH problem. Knowing the trapdoor a, we can efficiently decide whether or not $h_2 = g_2^a$. Now we set G to be the direct product $C \times C$. Then the input to the DDH problem is (x, y) where $x, y \in G$, that is, $x = (g_1, h_1)$ and $y = (g_2, h_2)$. It is obvious that (g_1, h_1, g_2, h_2) is a Diffie-Hellman quadruple if and only if y belongs to the subgroup $< x >$ of G generated by x. It follows that the DDH problem for the cyclic group C is equivalent to the subgroup membership problem of the group $H =< x >$, where $x = (g_1, g_1^a)$, in the group $G = C \times C =< g_1 > \times < g_1 >$.

Homomorphic Property: For any ciphertexts $c_1 = \epsilon(m_1)r_1$ and $c_2 = \epsilon(m_2)r_2$, where r_1, r_2 are outputs of $\mathcal{SAM}$ and m_1, m_2 are plaintexts in P, we have $c_1c_2 = \epsilon(m_1)r_1\epsilon(m_2)r_2 = \epsilon(m_1m_2)r_1r_2$ since ϵ is a homomorphism. Note also that $r_1r_2 \in H$. Therefore, c_1c_2 belongs to $\epsilon(m_1m_2)H$ and it is a ciphertext of m_1m_2. Thus the encryption function e is homomorphic. In the language of group

theory, the homomorphic property is a natural consequence of the quotient group G/H forms a group, that is, $c_1Hc_2H = c_1c_2H$ for all cosets c_1H, c_2H.

We summarize the mechanism of a homomorphic encryption in Fig. 1. The decryption d can be efficiently computed provided that the private key is given.

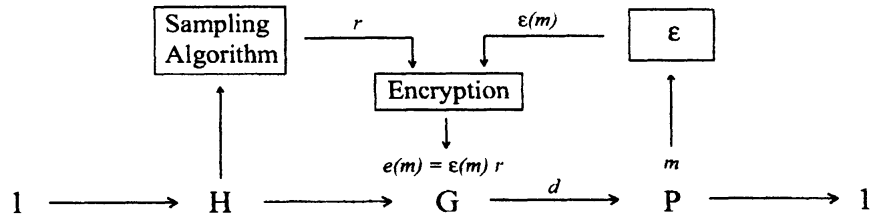

Figure 1: Exact Sequence and Mechanism of Homomorphic Encryption

ElGamal Encryption: Let $C = \langle g \rangle$ be a cyclic group of prime order p. Let $P = C$ and $G = C \times C$. The encoder ϵ is defined to be the function $m \rightarrow (1, m) \in G$. It is clear that ϵ is an isomorphism of P into G. Suppose that the public key for the ElGamal encryption is (g, g^b), where b is uniformly and randomly chosen. Let $H = \langle (g, g^b) \rangle$ the subgroup of G generated by the element (g, g^b). We note that $\epsilon(P) \cap H = 1$ and $G = \epsilon(P)H$. Recall that a ciphertext of $m \in P$ is $e(m) = (g^a, g^{ab}m) = (1, m)(g, g^b)^a = \epsilon(m)r$, where $r = (g, g^b)^a$ is randomly and uniformly chosen from the subgroup H of randomizers, that is, a is randomly chosen, and $e(m)$ belongs to $\epsilon(m)H$. Since ϵ is an isomorphism, the encryption is homomorphic, that is, $e(m_1m_2) = e(m_1)e(m_2)$, or $\epsilon(m_1m_2)H = \epsilon(m_1)H\epsilon(m_2)H$. The decryption $d : G \rightarrow P$ is defined by $(g^x, g^y) \rightarrow g^{-xb}g^y$. Clearly d is a homomorphism. Moreover, it is easy to see that Ker$d$ is H and $d \circ \epsilon = id_P$. Hence, we have the split exact sequence $1 \longrightarrow \langle (g, g^b) \rangle \longrightarrow C \times C \overset{\epsilon}{\curvearrowleft} C \longrightarrow 1$. We recall that the semantic security of the ElGamal is equivalent to the DDH problem [6].

Goldwasser-Micali Encryption: Let G be the subgroup of $(\mathbb{Z}/(N))^*$, where $N = pq$, consisting of the elements whose Jacobi symbol is 1, and H be the subgroup of G consisting of quadratic residues of G. Goldwasser-Micali encryption [2] is characterized as follows. Let P be the cyclic group of order two, that is, $(\mathbb{Z}/2, +)$. The encoder $\epsilon : P \rightarrow G$ is defined by $m \rightarrow g^m$, where g is an element of $G \setminus H$ and the public key. The decryption $d : G \rightarrow P$ is defined by $d(x) = 0$ if $x \in H$ and $d(x) = 1$ otherwise. The message $m \in P$ is encrypted to be $e(m) = g^m r = \epsilon(m)r$, where r is uniformly and randomly chosen from H. Clearly d is a homomorphism. Moreover, evidently Ker$d$ is H and $d \circ \epsilon = id_P$. Hence, we have the split exact sequence $1 \longrightarrow G^2 \longrightarrow G \overset{\epsilon}{\curvearrowleft} (\mathbb{Z}/2, +) \longrightarrow 0$. We recall that the semantic security of the Goldwasser-Micali is equivalent to the quadratic residue problem [2].

Benaloh encryption: Let p,q be two distinct primes. Set $N = pq$. Let n be a prime such that $n \mid \phi(N)(= (p-1)(q-1))$ and n and $\phi(N)/n$ are coprime. Set $G = (\mathbb{Z}/(N))^*$, $H = \{x^n | x \in G\}$ and $P = (\mathbb{Z}/(n), +)$. Choose $g \in G \setminus H$. The message $m \in P$ is encrypted to be $e(m) = \epsilon(m)r = g^m r \bmod N$, where r is uniformly and randomly chosen from H. For $w \in G$, the class of w, denoted by $[\![w]\!]_g$, is defined by the unique integer $x \in P$ for which there exists $y \in H$ such that

$g^x y \equiv w \bmod N$. The decryption function $d : G \to P$ is defined by $w \mapsto [\![w]\!]_g$. Clearly d is a homomorphism. Moreover, $\ker d = H$ and $d \circ \epsilon = id_P$. Hence, we have the split exact sequence

$$1 \longrightarrow G^n \longrightarrow G \overset{\epsilon}{\underset{d}{\rightleftarrows}} P \longrightarrow 0.$$

We recall that the semantic security of the Benaloh is equivalent to the the prime residuosity problem [1].

Okamoto-Uchiyama encryption: Let p,q be odd primes such that $|p| = |q| = k$. Set $n = p^2 q$ ($|n| = 3k$) and $G = (\mathbb{Z}/(n))^*$. Let Γ_p be the p-Sylow subgroup of G. A group homomorphism L_p of Γ_p into the additive group $(\mathbb{Z}/(p), +)$ is defined by $L_p(x) = (x-1)/p$. Choose $g \in G$ randomly such that the order of $(g^{p-1} \bmod p^2)$ is p. Let $h = g^n \bmod n$. Set $H = \{x^n | x \in G\}$ and $P = (\mathbb{Z}/(2^{k-1}), +)$. The encoder $\epsilon : P \to G$ is defined by $m \to g^m \bmod n$. The message $m \in P$ is encrypted to be $e(m) = \epsilon(m) r = g^m r \bmod n$, where r is uniformly and randomly chosen from H. The decryption function $d : G \to P$ is defined by $d(x) = L_p(x^{p-1} \bmod p^2)/L_p(g^{p-1} \bmod p^2) \bmod p$. Clearly d is a homomorphism. Moreover, $\ker d = H$ and $d \circ \epsilon = id_P$. Hence, we have the split exact sequence

$$1 \longrightarrow G^n \longrightarrow G \overset{\epsilon}{\underset{d}{\rightleftarrows}} P \longrightarrow 0.$$

Paillier encryption: Let p, q be odd primes. Set $n = pq$ and $G = (\mathbb{Z}/(n^2))^*$, $H = \{n\text{-th residues} \in G\}$ and $P = (\mathbb{Z}/(n), +)$. order $\phi(n^2) = n\phi(n)$. distinguishing n-th intractability hypothesis For $g \in G$, $\mathcal{E}_g : P \times (\mathbb{Z}/(n))^* \to G$ is defined by $(x, y) \mapsto g^x y^n \bmod n^2$. $\mathcal{E}_g$ is bijective if the order of g is a nonzero multiple of n. The set of the elements whose order is a nonzero multiple of n is denoted by $\mathcal{B}(\subset G)$. For $g \in \mathcal{B}$ and $w \in G$, the class of w, denoted by $[\![w]\!]_g$, is defined by the unique integer $x \in \mathbb{Z}/(n)$ for which there exists $y \in (\mathbb{Z}/(n))^*$ such that $\mathcal{E}_g(x, y) = w$. For $g \in \mathcal{B}$, the class function $w \mapsto [\![w]\!]_g$ is a homomorphism from G to $(\mathbb{Z}/(n), +)$. Set $\mathcal{S}_n = \{u < n^2 | u \equiv 1 \bmod n\}$. The function L on $\mathcal{S}_n$ is defined by $L(u) = (u-1)/n$. Choose a base $g \in \mathcal{B}$ randomly. The encoder $\epsilon : P \to G$ is defined by $m \mapsto g^m \bmod n^2$, The message $m \in P$ is encrypted to be $e(m) = \epsilon(m) r = g^m r \bmod n^2$, where r is uniformly and randomly chosen from H. The decryption function $d : G \to P$ is defined by $d(x) = L(x^\lambda \bmod n^2)/L(g^\lambda \bmod n^2) \bmod n$. Clearly d is a homomorphism. Moreover, $\ker d = H$ and $d \circ \epsilon = id_P$. Hence, we have the split exact sequence

$$1 \longrightarrow G^n \longrightarrow G \overset{\epsilon}{\underset{d}{\rightleftarrows}} P \longrightarrow 0.$$

It is shown in [5] that the the encryption scheme is semantically secure if and only if the *Decisional Composite Residuosity Assumption* is intractable.

Naccache-Stern encryption: Let σ be a square-free odd B-smooth integer, where B is a small integer and let n be a product of two distinct primes p, q such that $\sigma \mid \phi(n)$ and σ and $\phi(n)/\sigma$ are coprime. Let g be an element whose multiplicative order modulo n is a large multiple of σ. Set $G = < g >$, $H = \{x^\sigma | x \in \mathbb{Z}/(n)\}$ and $P = (\mathbb{Z}/(\sigma), +)$. The message $m \in P$ is encrypted to be $e(m) = \epsilon(m) r = g^m r \bmod n$, where r is uniformly and randomly chosen from H. The decryption function $d : G \to P$ is performed using the prime factors of σ and the Chinese Remainder Theorem.

Clearly d is a homomorphism. Moreover, $\ker d =< g^\sigma >$ and $d \circ \epsilon = id_P$. Hence, we have the split exact sequence

$$1 \longrightarrow G^\sigma \longrightarrow G \overset{\epsilon}{\underset{d}{\rightleftarrows}} P \longrightarrow 0.$$

We recall that the semantic security of the Naccache-Stern is equivalent to the the prime residuosity problem [3].

The textbook RSA has the homomorphic property, that is, $e(m_1 m_2) = (m_1 m_2)^e = m_1^e m_2^e = e(m_1)e(m_2)$. In this case, the space of plaintexts does not form a group unless the user restricts the domain of the plaintexts to $(\mathbb{Z}/n)^*$. Instead, usually the domain of the plaintexts is just the semigroup $\mathbb{Z}/n$. Thus, the textbook RSA is not characterized as the scheme above.

References

[1] J.Benaloh, Verifiable Secret-ballot Elections, PhD thesis, Yale University (1987)

[2] Goldwasser, S., Micali, S.: Probabilistic Encryption, *Jounal of Computer and System Sciences*, **28** (1984) 270–299

[3] Naccache,D., Stern, J.: A New Public-key Cryptosystem, Advances in Cryptology. (CRYPTO 1997) Lecture Notes in Computer Science, Vol. 1233. Springer-Verlag, (1997) 27–36

[4] Okamoto, T., Uchiyama, S.: A New Public-key Cryptosystem as Secure as Factoring, Advances in Cryptology (EUROCRYPT 1998) Lecture Notes in Computer Science, Vol. 1403. Springer-Verlag, (1998) 308–318

[5] Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, Advances in Cryptology (EUROCRYPT 1999) Lecture Notes in Computer Science, Vol. 1592. Springer-Verlag, (1999) 223-238

[6] Tsiounis, Y., Yung, M.: On the Security of ElGamal Based Encryption, Public Key Cryptography (PKC 1998) Lecture Notes in Computer Science, Vol. 1431. Springer-Verlag, (1998) 117–134

[7] Yamamura,A.: Homomorphic Encryptions of Sums of Groups, Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC 2007) Lecture Notes in Computer Science, Vol. 4851. Springer-Verlag, (2007) 357–366.

[8] Yamamura, A., Kurosawa, K.: Generic Algorithms and Key Agreement Protocols Based on Group Actions, Algorithms and Computation (ISAAC 2001) Lecture Notes in Computer Science, Vol. 2223. Springer-Verlag, (2001) 208–218

[9] Yamamura, A., Saito, T.: Private Information Retrieval Based on the Subgroup Membership Problem, Information Security and Privacy (ACISP 2001) Lecture Notes in Computer Science, Vol. 2119. Springer-Verlag, (2001) 206–220